Harris Corporation v. Huawei, et al **- Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
Exhibit G – U.S. Patent No. 7,440,572 ('572) – Claims 1, 47

Harris Corporation expressly reserves the right to supplement or modify these Disclosures as appropriate upon receipt of further information and discovery. The Huawei '572 Patent Accused Products (as that term is defined and the corresponding devices are identified in Harris's P.R. 3-1 and P.R. 3-2 disclosures cover pleading) infringe at least the following claims. References to instrumentalities in this chart are exemplary only and should not be construed as limiting the scope of any claim of the '572 patent. The Huawei '572 Patent Accused Products satisfy each claim element below literally. The Huawei '572 Patent Accused Products also satisfy claim elements under the Doctrine of Equivalents, including without limitation where specifically identified below, because they include and perform substantially similar functionality.

All ***bolded italics*** emphasis added unless noted otherwise.

'572 Patent Claim 1	Infringement By Huawei Corporation
1. A secure wireless local area network (LAN) device comprising:	The Huawei '572 Patent Accused Products infringe this claim. The Huawei '572 Patent Accused Products are secure wireless local area network (LAN) devices, and include the Huawei Zigbee Products. For example, and without limitation: Huawei is a "Promoter" level member of the Zigbee Alliance and produces products certified by Zigbee. *See, e.g.*, Zigbee Alliance, Our Members, *available at* https://www.zigbee.org/zigbeealliance/our-members/ (last accessed March 27, 2019); Zigbee Alliance, Zigbee Certified Products, *available at* https://www.zigbee.org/zigbee-products-2/#zigbeecertifiedproducts/?view_30_search=Huawei&view_30_page=1 (last accessed March 27, 2019) The Huawei Zigbee Products comply with the Zigbee standards, including the IEEE 802.15.4 standard (defining the Medium Access Control (MAC) and Physical (PHY) sublayers for Low-Rate Wireless Personal Area Networks (LR-WPANs) connectivity), which is the basis for the MAC and PHY layers in Zigbee certified products. *See, e.g.*, Zigbee Alliance, Zigbee 3.0, *available at* https://www.zigbee.org/zigbee-for-developers/zigbee-3-0/ (last accessed March 27, 2019); *see also* ZigBee Alliance, ZigBee Specification, Version r06 (June 27, 2005), at 17-18; ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 1 ("The IEEE 802.15.4 standard defines the two lower layers:

<table>
<tr><th>'572 PATENT CLAIM 1</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>

the physical (PHY) layer and the medium access control (MAC) sub-layer. The ZigBee Alliance builds on this foundation by providing the network (NWK) layer and the framework for the application layer.").

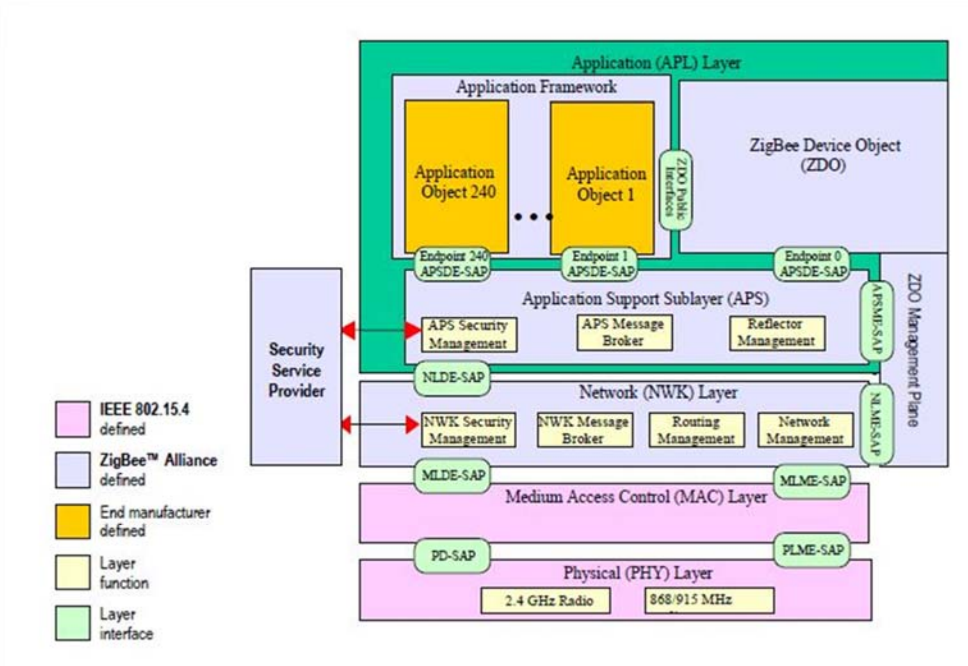


Figure 1 Outline ZigBee stack architecture

ZigBee Alliance, ZigBee Specification, Version r06 (June 27, 2005), at p. 18, Figure 1.

</td></tr>
</table>

’572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION

Huawei represents that certain of its products comply with and communicate according to the Zigbee standards. For example:

This topic introduces the wireless network access indicators of the ONT.

Table 9-1 Zigbee/Z-Wave access indicators

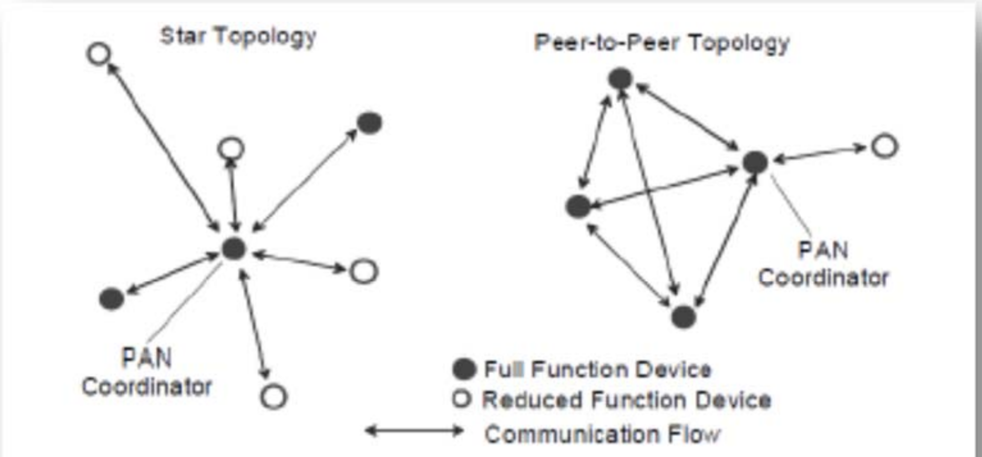
Indicator	Value(ZigBee)	Value(Z-Wave)
Standards compliance	IEEE 802.15.4 For ZHA1.2 and ZLL1.0 device management	ITU-T G.9959 For device plus management
Communication frequency	2.4GHz	• Australian standard: 908.4-916 MHz • U.S. standard: 919.8-921.42 MHz

Echolife ONT, Port Specifications, Jan. 24, 2019, at 10

> “The AR502 series IoT gateway is designed for industrial environments and supports communication in harsh environments such as extreme temperature, high humidity, and electromagnetic interference. The built-in industrial-grade LTE module supports high bandwidth, low-latency wireless access, and various local interfaces (RS485/RS422, RS232, Gigabit Ethernet and ZigBee) for connecting serial interface devices, Ethernet devices. The AR502 applies to multiple IoT fields, such as smart grid and smart transportation.”

Huawei AR502 Series IoT Gateway, Datasheet, at 2; *see also* Huawei AP7060DN Access Point Datasheet, *available at* https://e.huawei.com/us/related-page/products/enterprise-network/wlan/indoor-access-

Harris Corporation v. Huawei, et al - **Case No. 2:18-cv-439**
Plaintiff's Disclosure of Asserted Claims and Infringement Contentions (Pat. L.R. 3-1 & 3-2)
Exhibit G – U.S. Patent No. 7,440,572 ('572) – Claims 1, 47

'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	points/ap7060dn/wlan-ap7060dn (last accessed March 28, 2019), at 3; Huawei AR160-M Series Enterprise Routers Data Sheet, *available at* https://e.huawei.com/it/related-page/products/enterprise-network/routers/ar-agile/ar160-m/router_ar160-m, at 2. Zigbee and IEEE 802.15.4 standards describe and require a secure wireless local area network (LAN) device. For example, and without limitation:  **Figure 1—Star and peer-to-peer topology examples** IEEE Standard for Local and Metropolitan Area Networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Computer Society, IEEE Std 802.15.4-2011, at p. 9, Figure 1.

'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	"**device:** Any entity containing an implementation of the IEEE 802.15.4 medium access control and physical interface to the wireless medium. A device may be a reduced-function device or a full-function device." IEEE Std 802.15.4-2011, at p. 1. "A system conforming to this standard consists of several components. The most basic is the device. Two or more devices communicating on the same physical channel constitute a WPAN." IEEE Std 802.15.4-2011, at p. 8. "There are two device types: a full-function device (FFD) and a reduced-function device (RFD). The FFD may operate in three modes serving as a personal area network (PAN) coordinator, a coordinator, or a device. An RFD shall only operate as a device." IEEE Std 802.15.4-2011, at p. 18. "In a peer-to-peer topology, ***each device is capable of communicating with any other device within its radio communications range***. One device is nominated as the PAN coordinator, for instance, by virtue of being the first device to communicate on the channel." IEEE Std 802.15.4-2011, at p. 9. "An LR-WPAN device comprises at least one PHY, which contains the radio frequency (RF) transceiver along with its low-level control mechanism, and a MAC sublayer that provides access to the physical channel for all types of transfer. Figure 3 shows these blocks in a graphical representation, which are described in more detail in 4.4.1 and 4.4.2." IEEE Std 802.15.4-2011, at p. 11.

'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	"The PHY data service enables the transmission and reception of PHY protocol data units (PPDUs) across the physical radio channel. The general PHY requirements are described in Clause 8." IEEE Std 802.15.4-2011, at p. 11. "IEEE Standard for ***Local and metropolitan area networks***—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)" IEEE Std 802.15.4-2011, at p. i. "Keywords: ad hoc network, IEEE 802.15.4, low data rate, low power, LR-WPAN, mobility, PAN, personal area network, radio frequency, RF, short range, wireless, wireless personal area network, WPAN" IEEE Std 802.15.4-2011, at p. ii. "Solutions adopting the ZigBee standard will be embedded in consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor applications, toys, and games." ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 1. "This document contains specifications, interface descriptions, object descriptions, protocols and algorithms pertaining to the ZigBee protocol standard, including the application support sub-layer (APS), the ZigBee device objects (ZDO), ZigBee device profile (ZDP), the application framework, the network layer (NWK), and ***ZigBee security services***." ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 1.

'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	"**Access control list:** This is a table used by a device to determine which devices are authorized to perform a specific function. This table may also store the security material (for example, ***cryptographic keys***, frame counts, key counts, security level information) used for ***securely communicating with other devices***." ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 7. "To illustrate, wireless networks rely on the ability for autonomous devices to join a network and discover other devices and services on devices within the network. Device and service discovery are features supported within the device profile." ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 63. "The remaining portions of this document specify in greater detail the various security services available within the ZigBee stack. Basic definitions and references are given in clause 4.2. A general description of the security services is given in section 4.2.1. In this clause, the overall security architecture is discussed; basic security services provided by each layer of this architecture are introduced. Sections 4.2.2 and 4.2.3 give the ZigBee Alliance's security specifications for the Network (NWK) layer and the Application Support Sublayer (APS) layer, respectively. These clauses introduce the security mechanisms, give the primitives, and define any frame formats used for security purposes. Section 4.5 describes security elements common to the NWK and APS layers. Section 4.6 provides a basic functional description of the available security features. Finally, annexes provide technical details and test vectors needed to implement and test the cryptographic mechanisms and protocols used by the NWK and APS layers" ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 375.

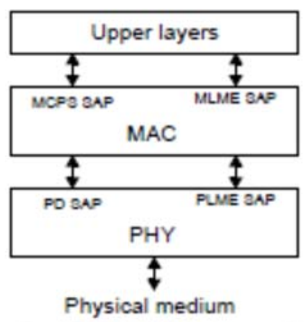
'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	"Where applicable, this architecture complements the security services that are already present in the IEEE Std. 802.15.4 [B1] security specification" ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 375. "*ad hoc* network devices" ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 376. "The features of the PHY are activation and deactivation of the radio transceiver, ED, LQI, channel selection, clear channel assessment (CCA), and transmitting as well as receiving packets across the physical medium." IEEE Std 802.15.4-2011, at p. 11.

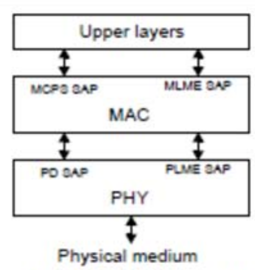
'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	5.1 MAC functional description The MAC sublayer handles all access to the physical radio channel and is responsible for the following tasks: — Generating network beacons if the device is a coordinator — Synchronizing to network beacons — Supporting PAN association and disassociation — Supporting device security — Employing the CSMA-CA mechanism for channel access — Handling and maintaining the GTS mechanism — Providing a reliable link between two peer MAC entities IEEE Std 802.15.4-2011, at p. 18

'572 PATENT CLAIM 1	**INFRINGEMENT BY HUAWEI CORPORATION**
	"Wireless personal area networks (WPANs) are used to convey information over relatively short distances. Unlike wireless local area networks (WLANs), connections effected via WPANs involve little or no infrastructure. This feature allows small, power-efficient, inexpensive solutions to be implemented for a wide range of devices. … This standard defines the physical layer (PHY) and medium access control (MAC) sublayer specifications for low-data-rate wireless connectivity with fixed, portable, and moving devices with no battery or very limited battery consumption requirements typically operating in the personal operating space (POS) of 10 m." IEEE Std 802.15.4-2011, at p. 1. "The cryptographic mechanism in this standard is based on symmetric-key cryptography and uses keys that are provided by higher layer processes. The establishment and maintenance of these keys are outside the scope of this standard. The mechanism assumes a secure implementation of cryptographic operations and secure and authentic storage of keying material." IEEE Std 802.15.4-2011, at p. 16.
[a] a housing;	The Huawei '572 Patent Accused Products are secure wireless local area network (LAN) devices which further contain a housing. For example, and without limitation: "Wireless personal area networks (WPANs) are used to convey information over relatively short distances. Unlike wireless local area networks (WLANs), connections effected via WPANs involve little or no infrastructure. This feature allows small, power-efficient, inexpensive solutions to be implemented for a wide range of devices.

'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	… This standard defines the physical layer (PHY) and medium access control (MAC) sublayer specifications for low-data-rate wireless connectivity with fixed, portable, and moving devices with no battery or very limited battery consumption requirements typically operating in the personal operating space (POS) of 10 m." IEEE Std 802.15.4-2011, at p. 1 "**device:** Any entity containing an implementation of the IEEE 802.15.4 medium access control and physical interface to the wireless medium. A device may be a reduced-function device or a full-function device." IEEE Std 802.15.4-2011, at p. 4. "The PAN coordinator will often be mains powered, while the devices will most likely be battery powered. Applications that benefit from a star topology include home automation, personal computer (PC) peripherals, games, and personal health care." IEEE Std 802.15.4-2011, at p. 9.

'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	 Huawei AR502 Series IoT Gateway, Datasheet, at 1; *see also* Huawei AP7060DN Access Point Datasheet, *available at* https://e.huawei.com/us/related-page/products/enterprise-network/wlan/indoor-access-points/ap7060dn/wlan-ap7060dn (last accessed March 28, 2019), at 1.  Huawei AR160-M Series Enterprise Routers Data Sheet, *available at* https://e.huawei.com/it/related-page/products/enterprise-network/routers/ar-agile/ar160-m/router_ar160-m, at 1.

'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
[b] a wireless transceiver carried by said housing;	The Huawei '572 Patent Accused Products infringe this claim. The Huawei '572 Patent Accused Products are secure wireless local area network (LAN) devices which further contain a wireless transceiver carried by said housing. For example, and without limitation: "An LR-WPAN device comprises at least one PHY, which contains the ***radio frequency (RF) transceiver*** along with its low-level control mechanism, and a MAC sublayer that provides access to the physical channel for all types of transfer." IEEE Std 802.15.4-2011, at p. 11.  **Figure 3—LR-WPAN device architecture** IEEE Std 802.15.4-2011, at p. 11, Figure 3.

'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	"**device:** Any entity containing an implementation of the IEEE 802.15.4 medium access control and physical interface to the wireless medium. A device may be a reduced-function device or a full-function device." IEEE Std 802.15.4-2011, at p. 4.
[c] a medium access controller (MAC) carried by said housing; and	The Huawei '572 Patent Accused Products infringe this claim. The Huawei '572 Patent Accused Products are secure wireless local area network (LAN) devices which further contain a medium access controller (MAC) carried by said housing. For example, and without limitation: "An LR-WPAN device comprises at least one PHY, which contains the radio frequency (RF) transceiver along with its low-level control mechanism, and ***a MAC sublayer that provides access to the physical channel for all types of transfer***." IEEE Std 802.15.4-2011, at p. 11.  **Figure 3—LR-WPAN device architecture** IEEE Std 802.15.4-2011, at p. 11, Figure 3.

'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	"**device:** Any entity containing an implementation of the IEEE 802.15.4 medium access control and physical interface to the wireless medium. A device may be a reduced-function device or a full-function device." IEEE Std 802.15.4-2011, at p. 4.
[d] a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver for encrypting both address and data information for transmission by at least adding a plurality of encrypting bits to both the address and the data information, and for decrypting both the address and the data information upon reception.	The Huawei '572 Patent Accused Products are secure wireless local area network (LAN) devices which further contain a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver for encrypting both address and data information for transmission by at least adding a plurality of encrypting bits to both the address and the data information, and for decrypting both the address and the data information upon reception. For example, and without limitation: "An LR-WPAN device comprises at least one PHY, which contains the ***radio frequency (RF) transceiver*** along with its low-level control mechanism, and a ***MAC sublayer*** that provides access to the physical channel for all types of transfer." IEEE Std 802.15.4-2011, at p. 11. "A device that implements security shall provide a ***mechanism for the MAC sublayer*** to ***provide cryptographic transformations on incoming and outgoing frames*** using information in the PIB attributes associated with security . . . ." IEEE Std 802.15.4-2011, at p. 131.

'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	"The inputs to this procedure are the frame to be secured and the SecurityLevel, KeyIdMode, KeySource, and KeyIndexparametersfrom the originating primitive or automatic request PIB attributes. ***The outputs from this procedure are the status of the procedure and, if this status is SUCCESS, the secured frame*.**" IEEE Std 802.15.4-2011, at p. 131. **7.2.1 Outgoing frame security procedure** The inputs to this procedure are the frame to be secured and the SecurityLevel, KeyIdMode, KeySource, and KeyIndex parameters from the originating primitive or automatic request PIB attributes. The outputs from this procedure are the status of the procedure and, if this status is SUCCESS, the secured frame. The outgoing frame security procedure involves the following steps: a) If the *macSecurityEnabled* attribute is set to FALSE and the SecurityLevel parameter is not equal to zero, the procedure shall return with a status of UNSUPPORTED_SECURITY. b) The procedure shall determine whether the frame to be secured satisfies the constraint on the maximum length of MAC frames, as follows: 1) The procedure shall determine the length AuthLen, in octets, of the Authentication field, AuthLen, from the SecurityLevel parameter and Table 58. 2) The procedure shall determine the length AuxLen, in octets, of the auxiliary security header, as described in 7.4, using KeyIdMode and the SecurityLevel parameter. 3) The procedure shall determine the data expansion as AuxLen + AuthLen. 4) The procedure shall check whether the length of the frame to be secured, including data expansion and FCS, is less than or equal to *aMaxPHYPacketSize*. If this check fails, the procedure shall return with a status of FRAME_TOO_LONG. c) If the SecurityLevel parameter is zero, the procedure shall set the secured frame to be the frame to be secured and return with a status of SUCCESS. d) The procedure shall set the frame counter to the *macFrameCounter* attribute. If the frame counter IEEE Std 802.15.4-2011, at p. 131.

<table>
<tr><th>'572 PATENT CLAIM 1</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>
"The procedure shall insert the auxiliary security header into the frame."

IEEE Std 802.15.4-2011, at p. 132.

7.4 Auxiliary security header

The Auxiliary Security Header field has a variable length and contains information required for security processing, including a Security Control field, a Frame Counter field, and a Key Identifier field. The Auxiliary Security Header field shall be present only if the Security Enabled field is set to one. The Auxiliary Security Header field shall be formatted as illustrated in Figure 62.

<table>
<tr><th>Octets: 1</th><th>4</th><th>0/1/5/9</th></tr>
<tr><td>Security Control</td><td>Frame Counter</td><td>Key Identifier</td></tr>
</table>
Figure 62—Format of the auxiliary security header

IEEE Std 802.15.4-2011, at p. 139.
</td></tr>
</table>

'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	(see below)

7.3.2 CCM* Nonce

The CCM* nonce is a 13-octet string and is used for the advanced encryption standard (AES)-CCM* mode of operation, as described in B.3.2. The nonce shall be formatted as shown in Figure 61, with the leftmost field in the figure defining the first (and leftmost) octets and the rightmost field defining the last (and rightmost) octet of the nonce.

Octets: 8	4	1
Source address	Frame counter	Security level

Figure 61—CCM* nonce

IEEE Std 802.15.4-2011, at p. 136.

> "The source address shall be set to the extended address *macExtendedAddress* of the device originating the frame, the ***frame counter to the value of the respective field in the auxiliary security header***, as defined in 7.4, and the security level to the value corresponding to the Security Level field, as defined in Table 58."

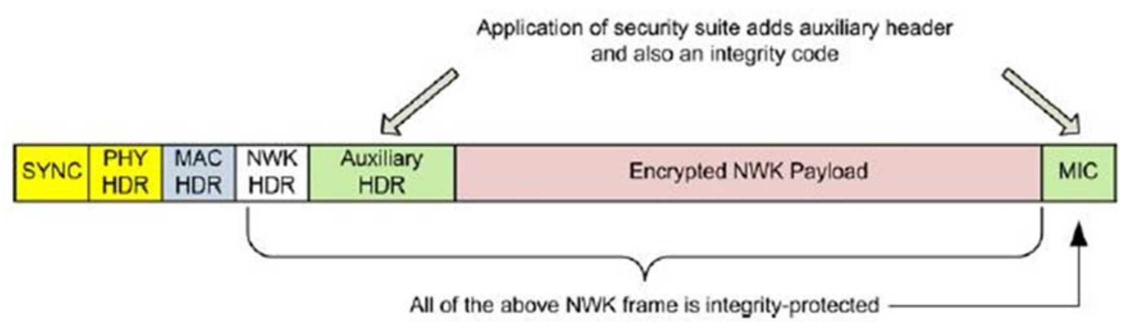
IEEE Std 802.15.4-2011, at p. 137.

> "***Securing a frame involves*** the use of the ***CCM* mode encryption*** and authentication transformation, as described in B.4.1. Unsecuring a frame involves the use of the CCM* decryption and authentication checking transformation, as described in B.4.2."

IEEE Std 802.15.4-2011, at p. 137.

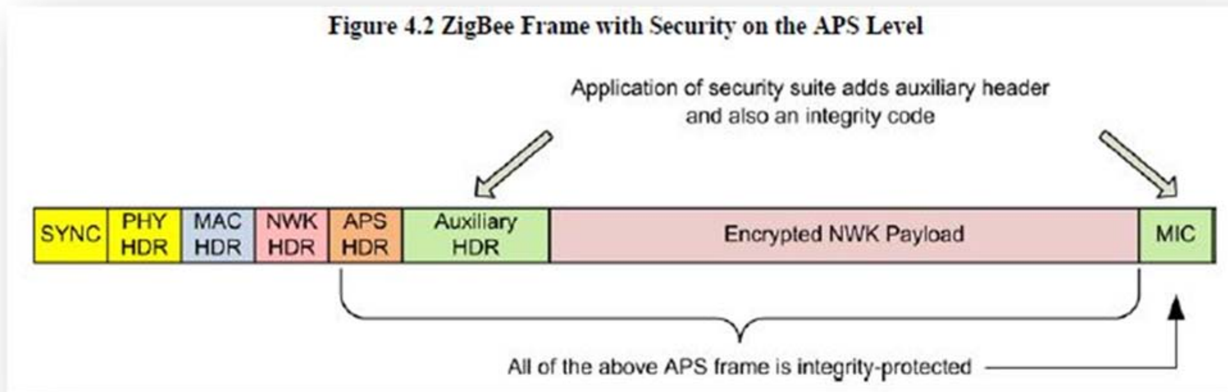
'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	7.3.4 CCM* transformation data representation This subclause describes how the inputs and outputs of the CCM* forward transformation, as described in B.4.1, are formed. The inputs are: — Key — Nonce — *a* data — *m* data The output is *c* data. IEEE Std 802.15.4-2011, at p. 137. "The Key data for the CCM* forward transformation is passed by the outgoing frame security procedure described in 7.2.1. The Nonce data for the CCM* transformation is constructed as described in 7.3.2." IEEE Std 802.15.4-2011, at p. 137.

'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	"**B.4.1 CCM* mode encryption and authentication transformation** . . . A bit string Key of length keylen bits to be used as the key. Each entity shall have evidence that access to this key is restricted to the entity itself and its intended key sharing group member(s)." IEEE Std 802.15.4-2011, at p. 230. "**B.4.2 CCM* mode decryption and authentication checking transformation** . . . A ***bit string Key of length keylen bits to be used as the key***. Each ***entity*** shall have evidence that access to this ***key*** is restricted to the ***entity itself*** and its ***intended key-sharing group member(s)***." IEEE Std 802.15.4-2011, at p. 232. "The ZigBee security architecture includes security mechanisms at two layers of the protocol stack. The NWK and APS layers are responsible for the secure transport of their respective frames. Furthermore, the APS sublayer provides services for the establishment and maintenance of security relationships. The ZigBee Device Object (ZDO) manages the security policies and the security configuration of a device. Figure 1.1 shows a complete view of the ZigBee protocol stack. The security mechanisms provided by the APS and NWK layers are described in this version of the specification." ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 378. "When a frame originating at the NWK layer needs to be secured ZigBee shall use the frame-protection mechanism given in section 4.3.1 of this specification, unless the SecurityEnable

'572 PATENT CLAIM 1	INFRINGEMENT BY HUAWEI CORPORATION
	parameter of the NLDE-DATA.request primitive is FALSE, explicitly prohibiting security. For example, no NWK layer security is used during transport of the NWK Key over the last hop to a joining device since APS security will be used to protect the frame. The NWK layer's frame-protection mechanism shall make use of the Advanced Encryption Standard (AES) [B8] and use CCM* as specified in Annex A. The security level applied to a NWK frame shall be determined by the *nwkSecurityLevel* attribute in the NIB." ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 378 Figure 4.1 shows an example of the security fields that may be included in a NWK frame. **Figure 4.1 ZigBee Frame with Security on the NWK Level**  ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 378, Figure 4.1 "When a frame originating at the APL layer needs to be secured, the APS sublayer shall handle security. The APS layer's frame-protection mechanism is given in section 4.4.1 of this

<table>
<tr><th>'572 PATENT CLAIM 1</th><th>INFRINGEMENT BY HUAWEI CORPORATION</th></tr>
<tr><td></td><td>
specification. The APS layer allows frame security to be based on link keys or the network key. Figure 4.2 shows an example of the security fields that may be included in an APL frame."

ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 379



ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 379, Figure 4.2

"If the APS layer has a frame, consisting of a header *ApsHeader* and payload *Payload*, that needs security protection and *nwkSecurityLevel* > 0, it shall apply security as follows:"

ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 387.

"The following caveat in these assumptions applies: due to the low-cost nature of *ad hoc* network devices, one cannot generally assume the availability of tamper-resistant hardware. Hence,
</td></tr>
</table>

'572 PATENT CLAIM 1	**INFRINGEMENT BY HUAWEI CORPORATION**
	physical access to a device may yield access to secret keying material and other privileged information, as well as ***access to the security software and hardware***." ZigBee Alliance, ZigBee Specification, Version r21 (Aug. 5, 2015), at 376.

'572 PATENT CLAIM 47	**INFRINGEMENT BY HUAWEI CORPORATION**
47. A method for providing a secure wireless local area network (LAN) comprising:	The Huawei '572 Patent Accused Products infringe this claim. The Huawei '572 Patent Accused Products include the Huawei Zigbee Products. The Huawei '572 Patent Accused Products provide a secure wireless local area network (LAN). For example, and without limitation: *See* Claim 1[preamble] above. The method further comprises the steps below.
[a] equipping a plurality of LAN devices with respective secure wireless LAN devices, each comprising a housing, a wireless transceiver carried by the housing, and a medium access controller (MAC) carried by the housing; and	The Huawei '572 Patent Accused Products equip a plurality of LAN devices with respective secure wireless LAN devices, each comprising a housing, a wireless transceiver carried by the housing, and a medium access controller (MAC) carried by the housing. For example, and without limitation: *See* claim elements 1[a] – [c] above. The method further comprises the steps below.

'572 PATENT CLAIM 47	INFRINGEMENT BY HUAWEI CORPORATION
[b] providing a cryptography circuit carried by the housing and cooperating with the MAC and the wireless transceiver for encrypting both address and data information for transmission, and for decrypting both address and data information upon reception.	The Huawei '572 Patent Accused Products provide a cryptography circuit carried by the housing and cooperating with the MAC and the wireless transceiver for encrypting both address and data information for transmission, and for decrypting both address and data information upon reception. For example, and without limitation: *See* claim element 1[d] above. > A device that implements security shall provide a ***mechanism for the MAC sublayer*** to ***provide cryptographic transformations on incoming and outgoing frames*** using information in the PIB attributes associated with security . . . . IEEE Std 802.15.4-2011, at p. 131. > The inputs to this procedure are the frame to be secured and the SecurityLevel, KeyIdMode, KeySource, and KeyIndexparametersfrom the originating primitive or automatic request PIB attributes. ***The outputs from this procedure are the status of the procedure and, if this status is SUCCESS, the secured frame***. IEEE Std 802.15.4-2011, at p. 131. > ***Securing a frame involves*** the use of the ***CCM* mode encryption*** and authentication transformation, as described in B.4.1. Unsecuring a frame involves the use of the CCM* decryption and authentication checking transformation, as described in B.4.2…. The ***Key data*** for the CCM* forward transformation is passed by the outgoing frame security procedure described in 7.2.1. IEEE Std 802.15.4-2011, at 137.